"We evaluated solutions from leading IT security market players as Cisco, Juniper, Symantec and others. When we tested the FortiGate-200B and then the FortiGate-300C devices, we were pleasantly surprised by the fact that these smaller and more affordable products had basically the same functionality as some larger models from other vendors."

*– Krešimir Miloslavić
 CISO
 Credit Bank Zagreb*

Credit Bank Zagreb (Kreditna banka Zagreb d.d.) chooses Fortinet to secure its Banking Transactions

Introduction
Credit Bank Zagreb is a 100% Croatian capital owned bank and is currently the 10th largest bank in Croatia. Credit Bank Zagreb has 23 branches and since 2009 has been one of the mostly rapidly growing banks in Croatia. The company is based in Zagreb.

Credit Bank Zagreb provides a range of banking services with deposit accounts and loans as its primary activities. It has expanded its operations with the acquisition of the credit bank of Concern Agram in 2006. Formed in 1992, Concern Agram regroups several companies, including Euroherc Osiguranje d.d., Jadransko Osiguranje d.d., Sunce Osiguranje d.d., Agram Life (life insurance) and Sunce Poliklinika (healthcare insurance). The whole group has a revenue of over 500 million US dollars.

The Challenge
Under the Basel II framework governing how the banking sector manages risks, IT security finally came to the forefront. Like in the rest of the world, cyber attacks have become one of the biggest problems facing the financial system in Croatia. Year after year, both the volume and level of sophistication of the attacks continue to increase. In response to this growing threat, Credit Bank Zagreb launched an effort to find a

Details
Customer Name: Credit Bank Zagreb
Industry: Financial/Banking
Location: Zagreb, Croatia

Challenges
- Credit Bank Zagreb needed to implement additional tools for proactive control of transactions and sessions.

Objectives
- The goal was to guarantee full security of Internet banking, with complete end-to-end traceability of all transactions and provide business continuity through disaster recovery sites.

Deployment
- FortiGate®-200As
- FortiGate-80Cs
- FortiGate-200Bs
- FortiGate-300C HA
- FortiGate-50Bs
- FortiGate-40C
- FortiGuard services

comprehensive security solution that could address all of its requirements. Credit Bank Zagreb handles yearly 3.5 million national payment transactions and 80 thousand foreign payment transactions. In 2011, the management team decided to implement additional tools for proactive control of transactions and sessions. The goal was to guarantee full security of Internet banking, with complete end-to-end traceability of all transactions and provide business continuity through disaster recovery sites.

The Solution

The project plan was prepared during 2008 and implementation started in 2009 with the acquisition of two FortiGate®-200As deployed in a High Availability (HA) configuration at their headquarters location. The project was later extended with two FortiGate-80Cs in order to separate external connections and offload VPN connections. It was followed by the purchase of additional FortiGate-200As and FortiGate-80Cs for the Disaster Recovery locations. The IT team of Credit Bank Zagreb is constantly working to improve the bank's security infrastructure. During 2012, the FortiGate-200A models were replaced with newer FortiGate-200Bs, and a new FortiGate-300C HA cluster was implemented as a central routing and security system. "We evaluated solutions from leading IT security market players as Cisco, Juniper, Symantec and others. When we tested the FortiGate-200B and then the FortiGate-300C devices, we were pleasantly surprised by the fact that these smaller and more affordable products had basically the same functionality as some larger models from other vendors. We needed BGP and OSPF routing, together with a good firewall, while implementing an Intrusion Prevention System (IPS) and content security, in an easily-deployed HA configuration. We have found all these features in the Fortinet solution, delivering a strong routing platform accompanied by strong security features", explained Krešimir Miloslavić, CISO at Credit Bank Zagreb. "We have also chosen Fortinet products for their price/performance ratio, high stability level and consolidation of multiple network security functions into a single device." The initial implementation was completed in 2010 with the critical functions of BGP routing, IPS and Denial of Service (DoS) protection activated. Krešimir Miloslavić continued: "Currently, in our main office in Zagreb we are using two FortiGate-200Bs and two FortiGate-80Cs as our

main firewall solution. We also have two FortiGate-300Cs to secure our Internet modules and ATM machines. In Zadar, for our back-up site, we implemented one FortiGate-200B and one FortiGate-80C. We are also using 20 FortiGate-50Bs as remote routers for ATM machines, which we are currently replacing with the newer FortiGate-40C models. We have also subscribed to Fortinet's FortiGuard services for Antivirus, Intrusion Protection, Web Filtering and Email Filtering for continuous protection against the latest threats." Today more than 200 employees in the main office as well as many remote locations of Credit Bank Zagreb are protected by Fortinet solutions.

The Benefits

With the adoption of Fortinet solutions, Credit Bank Zagreb was able to comply with the Basel II framework for IT security as well as optimize their IT infrastructure and benefit from a higher level of reliability. The new implementation has made the security infrastructure more manageable, flexible, robust and reliable.

The migration period went smoothly and without any major network security incidents. At the moment, there is only one network administrator responsible for the operation of the system. Fortinet devices are extremely easy to use for both monitoring and normal operations, allowing the bank to use its IT staff more efficiently.

"The implementation of Fortinet products completely met our expectations and requirements. The solutions are easy to manage on an everyday basis, and the staff did not need any additional training. Administration of the solution is minimal and system updates are infrequent. Our requirements were for a next-generation firewall solution and the Fortinet solution addresses exactly that part and more with its routing capabilities. In the future, we are planning to expand our security infrastructure with some new FortiGate-300Cs for the main firewall segment and some FortiGate-200Ds for VPN concentrators. In addition, there is also a project to implement FortiGate-40Cs for ATM machines in around 30 locations. We are also considering Fortinet's Web Application Firewall (WAF) and database protection solutions as a logical next step to improve the bank's network security even further," concluded Krešimir Miloslavić.

F⊏RTINET®

GLOBAL HEADQUARTERS	EMEA SALES OFFICE	APAC SALES OFFICE	LATIN AMERICA SALES OFFICE
Fortinet Inc.	120 rue Albert Caquot	300 Beach Road 20-01	Paseo de la Reforma 412 piso 16
899 Kifer Road	06560, Sophia Antipolis,	The Concourse	Col. Juarez
Sunnyvale, CA 94086	France	Singapore 199555	C.P. 06600
United States	Tel: +33.4.8987.0510	Tel: +65.6513.3730	México D.F.
Tel: +1.408.235.7700			Tel: 011-52-(55) 5524-8428
www.fortinet.com/sales			